Uitwerking puzzel 91-7: Je kunt het schudden

Het credit voor deze puzzel gaat naar Frans van Hoeve. Hij stuurde het ons, in een iets andere vorm, met titel 'Penny-flipping problem'. Hij was het tegengekomen in een leerboek voor de programmeertaal Simula67 met de titel *Simula Begin* (G.M. Birtwistle, 1973) en had het probleem opgelost en bewezen.
De formulering van de oorspronkelijke puzzel was:

> In een stapel van n munten ligt elke munt met kop naar boven. De operatie FLIP(m) op de stapel houdt in: Neem de bovenste substapel van m munten van de stapel, draai de substapel ondersteboven en zet hem terug op de overblijvende $n–m$ munten. We nemen een stapel van n munten en herhalen de operatiecyclus FLIP(1), FLIP(2), FLIP(3), ...FLIP(n), FLIP(1), FLIP(2), FLIP(3), ... ,tot alles weer met kop boven ligt.

Wij maakten wat variaties en veranderden de munten in kaarten om het draaien wat makkelijker te maken en voegden een nummering en positieve en negatieve zijden van de kaarten toe. Het inspireerde Harm Bakker, ondanks zijn mooie oplossing, tot bovenstaande dubbelzinnige titel. Wiskundig gezien was de puzzel niet eenvoudig, maar alle vragen konden worden beantwoord door de kaarten volgens de regels te schudden, dus empirisch. Zoals Jos Remijn schreef: 'Er hoeft niets te worden bewezen.' We geven eerst de antwoorden zonder bewijs. Bewijzen volgen als toegift.

We hadden een stapel van n kaarten die op tafel liggen. Ze zijn genummerd van 1 tot en met n. Op de achterzijde van de kaarten staan dezelfde nummers, maar dan negatief. We starten met alle kaarten voorzijde boven en op volgorde. Kaart nummer 1 ligt onderop de stapel en kaart nummer n bovenop.

Het schudden gaat als volgt:
We pakken de bovenste kaart van de stapel, draaien hem ondersteboven en leggen hem terug. Daarna pakken we in één greep de 2 bovenste kaarten, draaien ze samen ondersteboven en leggen ze zo terug. De bovenzijde van de bovenste kaart heeft dan waarde $1–n$, dus negatief. Daaronder hebben we kaart nr. n, met waarde aan de bovenzijde $+n$. We gaan zo door met draaien, steeds een kaart meer, tot we als laatste de hele stapel ondersteboven draaien. Dit is één ronde en daarna gaan we door met een nieuwe ronde, op dezelfde manier als de eerste keer.
We stoppen wanneer alle kaarten weer met de positieve zijde boven liggen.
We willen weten hoe lang dat duurt en ook in welke volgorde de kaarten dan liggen.

Enkele definities:

- n = aantal kaarten.
- k = kaartnummer ($1 \le k \le n$).
- w = waarde, het getal op de bovenliggende zijde van de kaart. Als de kaart met de positieve zijde boven ligt geldt $w = k$, anders $w = –k$, dus $–n \le w \le n$.
- p = plaatsnummer van de kaarten in de stapel, te beginnen met de onderste kaart op $p = 1$ en de bovenste op $p = n$.
- r = aantal hele rondes dat is uitgevoerd.
- $d(n)$ = het aantal keren dat we moeten draaien tot alle w weer positief zijn, dus alle kaarten met de positieve zijde boven.
- C = aantal hele rondes dat we zouden moeten uitvoeren totdat de eerste kaart weer onder ligt, hetzij met de positieve zijde boven, hetzij met de negatieve zijde boven.
- a = de waarde van de onderste kaart op het moment dat een nieuwe ronde begint.

We gaven, voorafgaand aan de opgaven, zonder bewijs een aantal observaties die we hieronder in het kort herhalen, met enkele toelichtingen.

OBSERVATIES:

a) De kaartnummers *k* die we achtereenvolgens aan het eind van een heel aantal rondes op een bepaalde plaats *p* in de stapel zien, doorlopen een zekere cykel. De periode (lengte) van die cykels is niet per se op elke plaats in de stapel even groot. Voor de $p = 1$ is dat *C*. Op andere plaatsen blijken de periodes of even lang, of korter dan *C*, maar altijd een deler van *C*. Dus na *C* hele rondes liggen alle kaarten weer op de oorspronkelijke plaats.

b) Steeds is *C* het kleinste natuurlijke getal > 0 waarvoor geldt: $2^C \equiv \pm 1$ modulo *N*. Daarbij is $N = g(n)$ een functie van *n*.

c) $d(n) = n \times C$ of $n \times C – 1$. Met andere woorden: Alle kaarten liggen weer met de positieve zijde boven aan het eind van een hele ronde, of één draai eerder.

d) Afbeeldingen: Voor elke *n* geldt: Er bestaan getallen *s* en $m > n$, zodanig dat alle cykels die we zien bij *n* kaarten ook bij *m* kaarten voorkomen, maar dan met waarden en dus ook kaartnummers overal *s* keer zo groot.

We vonden het voor het uitschrijven van de getallen op de kaarten overzichtelijker om ze naast elkaar op te schrijven, met links de onderste kaart ($p = 1$) en rechts de bovenste ($p = n$). Voor het uitproberen met echte kaarten is een stapel wel handiger.

Opgave 1: Bepaal $d(n)$ voor $n = 3$, 4 en 5.
Voor $n = 3$ schrijven we de waarden *w* van het hele proces uit:

start situatie :	1, 2, 3;		
1e ronde:	1, 2, –3;	1, 3, –2;	2, –3, –1;
2e ronde:	2, –3, 1;	2, –1, 3;	–3, 1, –2;
3e ronde:	–3, 1, 2;	–3, –2, –1;	1, 2, 3;

$d(n)=9$. We zien bovendien dat de kaarten weer op volgorde liggen met 1 onder.

$n = 4$: $d(4) = 11$, dat zijn 3 hele rondes min één keer draaien. De kaarten liggen nu in omgekeerde volgorde met 4 onder en 1 boven.
$n = 5$: $d(5) = 24$. Dat zijn 5 hele rondes min één keer draaien. De kaarten liggen ook hier in omgekeerde volgorde met 5 onder en 1 boven.
U kon dit vinden door het uit te voeren met een stapeltje kaarten, of met behulp van de resultaten van opgave 4.

Voor opgave 2 letten we alleen op de plus- en mintekens van de bovenzijden van de kaarten na een geheel aantal rondes voor stapels van $n = 2^i$ of $n = 2^i – 1$ kaarten. Vraag 2a kon worden opgelost door het met uw stapeltje kaarten uit te proberen. En dat geeft dan een vermoeden voor het antwoord op 2b.
Opgave 2a: We onderzoeken dit voor $n = 4$, 7 en 8.

	$n = 2^2 = 4$	$n = 2^3 – 1 = 7$	$n = 2^3 = 8$
start:	+ + + +	+ + + + + + +	+ + + + + + + +
na 1e ronde:	+ + – –	+ + + – – – –	+ + + + – – – –
na 2^e ronde:	+ – + –	+ – – + + – –	+ + – – + + – –
na 3^e ronde:	– – – –	– + – + – + –	+ – + – + – + –
na 4^e ronde:		+ + + + + + +	– – – – – – – –

Bij $n = 4$ en $n = 8$ dus afwisselend even lange rijtjes plussen en minnen, waarbij de lengte van die rijtjes elke ronde halveert, zodat je na *i* rondes steeds om-en-om plussen en minnen krijgt, en na $i+1$ rondes ofwel allemaal plussen ofwel allemaal minnen. Bij $n = 7$ is het eerste rijtje steeds één korter dan de andere.

Opgave 2b: Wat is in het algemeen de waarde van $d(n)$ als $n = 2^i$ of $2^i – 1$?
We zagen al dat na $i+1$ rondes alle tekens gelijk zijn. Bij $n = 2^i – 1$ zijn ze allemaal positief, dus

$d(2^i - 1) = (2^i - 1)\cdot(i+1)$. Bij $n=2^i$ zijn ze na $i+1$ rondes allemaal negatief. Maar dan waren ze één draai eerder allemaal positief, immers bij de laatste draai van een ronde worden alle kaarten omgekeerd.
Gevolg: $d(2^i) = (2^i)\cdot(i + 1)-1$.

In opgave 3 letten we alleen op de kaartnummers, dus niet per se of de positieve kant boven of onder ligt. Ook dit kunnen we empirisch oplossen en dan een vermoeden formuleren.

Opgave 3a: Onderzoek bij welke waarden van n er een kaart is die na de eerste hele ronde weer op dezelfde plaats in de stapel ligt. Natuurlijk ligt die kaart na elke volgende hele ronde dan ook weer op diezelfde plaats. Enig gedraai levert op:
$n = 1 (k = 1)$, $n = 4$ $(k = 3)$, $n = 7 (k = 5)$, $n = 10$ $(k = 7)$, $n = 13$ $(k = 9)$ enzovoort.
Vermoeden: Bij $n = 3t + 1$ of, wat hetzelfde is: $2n + 1 = 3s$. Dan blijft de kaart op $p = n-t = (2n + 1)/s$ op z'n plaats.

Opgave 3b: Idem voor perioden van lengte 2.
Dat is het geval wanneer twee kaarten per ronde van plaats worden verwisseld.
We vinden: $n = 2$ (1 en 2), $n = 7$ (3 en 6), $n = 12$ (5 en 10), $n = 17$ (7 en 14) enzovoort.
Vermoeden: als $n = 5t + 2$ dus $2n + 1$ is een 5-voud. Dan staan de kaarten op plaatsen $p = n-t$ en $p = 2t+1$ na twee rondes weer op hun plek.

We kijken nu naar de waarden w aan het eind van elke ronde, dus negatief als de kaart op z'n kop ligt.
Opgave 4a: Bepaal een of meerdere functies $f_n(w)$ die de permutatie bepaalt van de waarden w. Dus als w een waarde op een bepaalde plaats in de stapel is, dan is $f_n(w)$ de waarde die daar één ronde later ligt. Een paar voorbeelden:

	$n = 4$	$n = 13$												
$r = 0$:	+1 +2 +3+4;	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13
$r = 1$:	+2 +4 –3–1;	+2	+4	+6	+8	+10	+12	–13	–11	–9	–7	–5	–3	–1
$r = 2$:	+4 –1 +3–2;	+4	+8	+12	+11	–7	–3	+1	+5	+9	+13	–10	–6	–2
$r = 3$:	–1 –2 –3–4;	+8	–11	–3	–5	+13	–6	+2	+1	–9	–1	–7	–12	–4

Vermoeden na de eerste ronde: Daar liggen eerst alle positieve even nummers, gevolgd door alle negatieve oneven nummers, beide van klein naar groot. Dan zien we dat voor de linkerhelften geldt: $f = 2w$, de waarden worden verdubbeld. Rechts zien we : $f = 2w - (2n + 1)$.
Voor elke kaart geldt dus $f_n(w) = 2w$ modulo$(2n + 1)$, met $-n \leq f_n(w) \leq +n$. Maar dat klopt ook voor alle volgende rondes.
Opgave 4b: Bepaal de N uit observatie b als functie van n. Observatie b gaat over de waarde van C, de lengte van de cykel van kaartnummer 1.
Voor alle rondes geldt dus $f_n(w) \equiv 2w \bmod (2n + 1)$. Als we niet 1, maar C rondes hebben doorlopen, dan geldt dus voor de onderste kaart: $w = 2^C$ modulo $(2n + 1)$, met $-n \leq w \leq +n$.
En C is het kleinste positieve getal waarvoor $2^C \equiv \pm 1 \bmod(N)$, dus met $N = 2n + 1$ kunnen we zo C bepalen en is de cykellengte van de eerste kaart gelijk aan C.

Opgave 5a: Gevraagd werd om observatie d te controleren voor $n = 4$ en $m = 13$, en om de bijbehorende waarde van s te bepalen. We geven nog eens de resultaten aan het eind van de eerste 3 rondes voor stapels van 4 en 13 kaarten.
Alle vier de kolommen van de stapel met $n = 4$ (rood) worden afgebeeld op de rode kolommen van de stapel met $m = 13$, steeds 3 keer zo groot als bij $n = 4$. Na de 2^{e} ronde herhalen de rood aangegeven waarden zich met alleen verandering van teken. Dus $s = 3$.

	n=4				n=13												
r=0:	+1	+2	+3	+4;	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13
r=1:	+2	+4	–3	–1;	+2	+4	+6	+8	+10	+12	–13	–11	–9	–7	–5	–3	–1
r=2:	+4	–1	+3	–2;	+4	+8	+12	+11	–7	–3	+1	+5	+9	+13	–10	–6	–2
r=3:	–1	–2	–3	–4;	+8	–11	–3	–5	+13	–6	+2	+1	–9	–1	–7	–12	–4

Opgave 5b: Nu moeten we nagaan voor welke waarden van s en m dit bij gegeven n in het algemeen het geval is. Het antwoord is: als $M = 2m + 1$ deelbaar is door $N = 2n + 1$, dan $s = M/N$.

Verklaringen en bewijzen: Enkele inzenders hebben zich hier met succes aan gewijd.

Eerst opgave 5:

Passen we op het voorbeeld $n = 4$ en $m = 13$, uit opgave 5a de formule uit opgave 4 toe dan hebben we voor n: $f_n(w) \equiv 2w \bmod(N)$ en voor m: $f_m(v) \equiv 2v \bmod(M)$, met $N = 2n + 1 = 9$ en $M = 2m + 1 = 27$.

In het algemeen geldt dat als $x \equiv y \bmod z$ ook geldt $s \cdot x \equiv s \cdot y \bmod(s \cdot z)$, want als y de rest is bij de integerdeling $z \backslash x$ dan is $s \cdot y$ de rest bij de integerdeling $s \cdot z \backslash (s \cdot x)$. Dus als $v = 3w$, dan ook $f_m(v) = 3f_n(w)$

en dus is de kolom $3p$ bij m 'gelijkvormig' aan die van p bij n.

Bij gegeven n zoeken we dus waarden van m, zodat $M = sN$. Omdat M altijd oneven is, is s dat ook. Bij een gegeven waarde van n vinden we dus bij elk oneven getal s een oplossing.

We gaan eerst de gevonden formule $f_n(w) \equiv 2w \bmod(2n + 1)$ bewijzen. Daarmee kunnen we namelijk alle andere resultaten afleiden.

In de formule is w de waarde van de kaart op een bepaalde plaats p in de stapel na een heel aantal rondes, en $f_n(w)$ de waarde op die plaats één ronde later.

De permutatie van de kaarten per ronde:

We kunnen ons het resultaat van het draaien van een hele ronde voorstellen door de kaarten van links naar rechts naast elkaar op tafel te leggen en met een lang stuk plakband aan elkaar te plakken. Die sliert kaarten rollen we dan van rechts naar links op, tot ten slotte de kaart die eerst onderop lag ($p = 1$) dan bovenop ligt. De laatste kaart n komt zo in het midden. We zien dan dat alle kaarten die op even plaatsen lagen nu onderop liggen, in volgorde te beginnen met de kaart van plaats 2. Daarna volgen de kaarten die op oneven plaatsen lagen, in volgorde, maar van de laatste tot de eerste. Bovendien zijn daarbij precies alle kaarten die op oneven plaatsen lagen omgekeerd.

Bewijs formule: Op de plaats waar aan het eind van een hele ronde waarde w ligt, ligt een ronde later $2w \bmod (N)$, waarbij $N = 2n + 1$. Dus $f_n(w) \equiv 2w \bmod (2n + 1)$, met $-n \leq f_n(w) \leq +n$.

Als we het boven beschreven resultaat van 'oprollen' bekijken voor alle waarden w aan het eind van de eerste ronde, dan komt dat overeen met de genoemde formule. Bij de start ($r = 0$) is op plaats p de waarde w gelijk aan p. Daarna ($r = 1$) is die waarde gelijk aan $f_n(p)$, dus ook $f_n(w)$. Dus voor de eerste ronde is de formule correct. Nu moeten we nog aantonen dat dat ook zo is bij de volgende rondes.

We schrijven zoals we al eerder deden de waarden na elke ronde op in een matrix waarin de rijen de toestand aangeven steeds aan het eind van een ronde. Kijken we naar de absolute waarden (de kaartnummers), dan is rij $r = 1$ een bepaalde permutatie van rij 0. Omdat we elke ronde dezelfde handelingen uitvoeren krijgen we de kaartnummers van rij 2 door dezelfde permutatie uit te voeren op rij 1 enzovoort. Als we het aantal rijen genoeg uitbreiden krijgen we dus in elke kolom een cykel van kaartnummers. Diezelfde cykel komt in meerdere kolommen voor, steeds met een ander kaartnummer bovenaan. Als in die cykel kaart p gevolgd wordt door kaart q dan worden de bewegingen van kaart p één ronde later gevolgd door dezelfde bewegingen van kaart q. En dus als kaart p bij die beweging wordt omgedraaid, gebeurt datzelfde met kaart q in de volgende ronde. Het teken van de waarden van 2 kaarten die elkaar opvolgen in zo'n cykel is dus ofwel altijd gelijk ofwel altijd verschillend.

En dat betekent dat als op plaats p na 2 opvolgende rondes de waarden w en v liggen, er een andere plaats is waar in de beginstand en na één ronde ofwel de waarden w en v, ofwel de waarden $-w$ en $-v$ lagen. Dus ofwel $v = f_n(w)$ ofwel $-v = f_n(-w)$ wat in beide gevallen resulteert in $v = f_n(w)$, en dus geldt de formule voor alle rondes.

Een belangrijke gevolg van de formule $f_n(w) \equiv 2w \bmod(N)$:
Als we alle waarden w die verschijnen na een heel aantal rondes in onze matrix noteren, met rijen r en kolommen p, dan geldt in kolom p : $w = p \cdot 2^r$ en per rij r: $w = a \cdot p$, met $a = 2^r$, het eerste getal in rij r. Alles natuurlijk modulo $2n + 1$ volgens afspraak.
We kunnen zo dus alle waarden na r rondes rechtstreeks berekenen.

Bewijs observaties a en b:
In observatie a is C de cykellengte van de kaartnummers op plaats $p = 1$. Het kaartnummer is de absolute waarde van de waarde w. Na C rondes hebben we dus op plaats 1 de waarde ±1, en uit $w = p \cdot 2^r$ volgt dan $\pm 1 \equiv 2^C \bmod N$.
Op plaats p hebben we dan na C rondes: $w \equiv p \cdot 2^C \bmod N \equiv \pm p \bmod N$, en omdat $0 < p \leq n$ wordt dat $w = \pm p$, met hetzelfde teken als de waarde in kolom 1. Dus elke kaart ligt dan weer op de oorspronkelijke plaats en ze hebben allemaal hetzelfde teken, plus of min. De cykellengte van die kaarten is dus in elke kolom gelijk aan C of kleiner, maar is dan in elk geval een deler van C.
Omdat dit resultaat altijd optreedt als in een bepaalde ronde r geldt $\pm 1 \equiv 2^r \bmod N$ is C (observatie b) het kleinste getal waarvoor dit geldt.

Verklaring van de patronen van plussen en minnen die we zien als $n = 2^i$ of $n = 2^i - 1$ (opgave 2).
We kunnen wat er gebeurt in elke ronde ook als volgt beschrijven: om-en-om worden de kaarten op 2 stapeltjes gelegd. Het stapeltje met de oneven kaarten wordt dan omgekeerd op het stapeltje met de even kaarten gelegd. We hebben dan onderin kaarten met positieve waarde, bovenin kaarten met negatieve waarde.
Bij de 2e ronde krijgen we eerst 2 stapeltjes met onderin positief, bovenin negatief. Na omdraaien en op elkaar leggen krijgen we 4 delen, afwisselend positief en negatief. Zolang die delen allemaal meer dan één kaart bevatten gaat dat zo door.
Als $n = 2^i$ blijven alle delen steeds even lang tot ze allemaal precies 1 kaart hebben. Dan zijn de waarden afwisselend positief en negatief, de onderste positief. In de volgende ronde komen dan alle kaarten kop onder.
Als $n = 2^i - 1$ bevat het onderste deel steeds één kaart minder dan de rest. Je eindigt dan met de waarden afwisselend positief en negatief, maar de onderste kaart is negatief. Na de laatste ronde ligt alles nu dus kop boven.

Verklaring observatie c
We weten al dat na C rondes alle waarden eenzelfde teken hebben. Als die waarde positief is liggen dus alle kaarten kop boven na $n \cdot C$ keer draaien. Als die waarde negatief is lagen vlak voor het eind van de vorige ronde, vóórdat de hele stapel werd omgekeerd, alle kaarten kop boven, dus na $n \cdot C - 1$ keer draaien.
Na $C \cdot n$ of $C \cdot n - 1$ keer draaien liggen dus alle kaarten met de positieve zijde boven.
De vraag is nog of dat ook eerder kan gebeuren.
Stel dat dat gebeurt tijdens een ronde die start met waarde $w = a$ op plaats $p = 1$, en dat in die ronde na een aantal keer draaien alle waarden positief zijn.
Als we dan terug redeneren wat de tekens zijn geweest bij de start van die ronde, dan kunnen we nagaan dat er, van onder naar boven in de stapel, eerst een aantal (i) kaarten positief waren (die zijn nooit omgekeerd) en dat de laatste $n - i$ kaarten daar om en om – en + op volgen.
Vervolgens willen we weten óf dit kan gebeuren, en zo ja, welke waarde a er dan bij het begin van die ronde op plaats 1 moet hebben gelegen.

Met a op plaats 1 weten we dat de waarden van de kaarten bij de start van die ronde van onder naar boven waren: a, $2a$,$3\,a$, ..., $n{\cdot}a$, alles modulo $2n+1$. Maar we zijn alleen geïnteresseerd in de tekens + of – en dat kunnen we opzoeken in onderstaand tekenschema van de functie $w(x) \equiv x \bmod(2n+1)$, met $|w| \leq n$. We hebben alleen de positieve x-as nodig, want voor deze functie geldt: $w(x) = -w(x)$.



De gebieden waar $w > 0$ zijn zwart gekleurd en rood waar $w < 0$. Die gebieden bevatten elk n roosterpunten, en zijn afwisselend zwart en rood. Vóór elk zwart gebied zit een 'gaatje' als x een veelvoud is van $2n+1$, dan is $w = 0$ en komt niet voor. Als we de gebieden nummeren van links naar rechts, te beginnen met gebied $g = 1$, dan zijn de oneven gebieden zwart, de even rood.
We plaatsen nu de reeks getallen a, $2a$, $3a$, ..., $n{\cdot}a$ op de x-as van dit tekenschema. De onderlinge afstand tussen die punten is steeds a. En omdat $|a| \leq n$ en elk gebied n getallen bevat, kan er nooit een gebied worden overgeslagen. Met $a = n$ liggen daarom alle waarden in de gebieden $g = 1$ tot en met n, elk precies één. De reeks is dan afwisselend +, –, dus $i = 1$. En met $a = -n$ afwisselend –,+, dus $i = 0$.
En ook weten we nu: Alleen als $a = 1$ ligt de hele reeks in gebied $g = 1$ en is alles positief. Merk ook op, dat de onderste kaart pas wordt omgedraaid na n keer draaien en moet dus bij de eerste n–1 draaibeurten al positief zijn geweest.
Voor het geval dat in een bepaalde ronde na een zeker aantal draaien alles positief wordt, kunnen we nu een tabel maken wat dan i en a zijn geweest aan het begin van die ronde.

draai	0	1	2	3	.....	*n-1*	*n:*
i	*n*	$n-1$	$n-2$	$n-3$	…..	1	0
a	1	>0	>0	>0	….	*n*	$-n$

Voor de draaien 1 tot en met $n-2$ is $1 < i < n$ en moeten dus in elk geval a en $2a$ in gebied $g = 1$ liggen, dus $2a \leq n$ zodat $a \leq n/2$. Maar, dan liggen er in gebied $g = 2$ ook minstens 2 getallen en is het einde van die reeks niet afwisselend –,+ .
De gezochte positieve kaarten kunnen we dus alleen vinden als $i = n$, $i = 1$ of $i = 0$ en dus $a = 1$ of $a = \pm n$ bij de start van een ronde, dus aan het eind van de ronde daarvoor.
$a = 1$: We wisten al dat $a = 1$ te vinden is na ronde 0 en dan pas weer aan het eind van ronde C of zelfs $2C$.
$a = n$: We moeten dan $n-1$ keer draaien. Maar een ronde later hebben we $a= -1$, dus in ronde C.
$a = -n$: Dan moeten we n keer draaien en een ronde later hebben we $a = 1$, ook in ronde C.
Voor die drie gevallen vinden we dan $d(n) = C \cdot n$ of $C \cdot n-1$ en levert geen eerdere toestanden op waar alle kaarten met de positieve zijde boven liggen. Daarmee is observatie c bewezen.

<u>De afbeeldingsstelling,</u> en daarmee observatie d, hebben we al bewezen na opgave 5b.
Maar wat kunnen we hier mee?
Bijvoorbeeld:
Neem n = 1, dus N = 3. Die heeft alleen een cykel van lengte 1. Die 1-cykel van $n = 1$ wordt dus afgebeeld op alle m waarvoor $2m+1$ een 3-voud is (opgave 3a).
Evenzo, als M deelbaar door 5, dan wordt $n = 2(N = 5)$ met twee 2-cykels daar op afgebeeld (opgave 3b).
Verder: Met n kaarten, waarbij N niet priem is, dan is $C < n$. Dat mogen we echter niet omdraaien: Als N priem, dan wil dat niet zeggen dat $C = n$. Zie bijvoorbeeld $n = 8$, met $N = 17$ en $C = 4$.

Wel bewees Gerard Bouwhuis dat als *N* priem is, dan zijn alle cykels even lang!